REMARKS

I. Introduction

In response to the Office Action dated October 6, 2003, please consider the following remarks. Claims 1-8 and 10-19 remain in the application. Re-examination and re-consideration of the application, as amended, is requested.

II. The Cited References and the Subject Invention

A. The Benson Reference

European patent applications EP 0 936 530 (hereinafter the Benson reference) discloses a virtual smart card. The virtual smart card emulates a real smart card by providing identical interface and services. The virtual smartcard has no physical manifestation and any smartcard-aware application can seamlessly interface with either a real smartcard or the virtual smartcard. A virtual smartcard server or duplication-protected physical media communicates with the virtual smartcard in order to activate or deactivate the virtual smartcard.

B. The Gabrielle Reference

"USB Forum Produces Logo, Awareness Initiative" by Gabrielle C. Mitchell, Computer Retail Week 1997, n. 192, pg. 49 (hereinafter, the Benson reference) is a news story about the use of USB-compliant devices.

C. The Subject Invention

The Applicants' invention is a compact, self-contained, personal key. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system. Importantly, the token comprises (1) a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol, and (2) an interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-

-7-

G&C 30074.27-US-I1

compliant messages into USB-compliant messages. These features provide specific advantages described in the Applicants' specification:

> First, smartcard processors 320 are relatively inexpensive and readily available. Second, a large number of application programs 110 have been developed for the use of smartcards, including the personal computer/smartcard (PC/SC) interface developed by the MICROSOFT CORPORATION. By providing a smartcard processor (which complies with the smartcard I/O protocols and supports smartcard command sets), this software can be used with a personal key 300 in a USB-compliant form factor. (Specification, page 10, lines 1-7)

E. Differences Between the Subject Invention and the Cited References

The Benson reference discloses a virtual smartcard, i.e. *software*, running on a general purpose processor, that emulates the behavior of a smartcard. The Applicants' invention, in contrast, uses a *physical* smartcard processor.

The Applicants' invention translates smartcard commands to USB packets (on the computer) and translates the received USB packets back to smartcard commands in the token. The virtual smartcard (VSC) disclosed in the Benson reference does not send commands at all ... it receives smartcard commands and executes them using a software emulation.

The VSC reader described in the Benson reference does not package or translate smartcard commands, it merely forwards them unchanged to the VSC software. The Applicants' virtual reader packages smartcard commands to a USB format and sends them to the USB token, where the commands are unpacked and executed by a real smartcard processor.

With the foregoing differences in mind, the Applicants respectfully request that the following remarks be considered.

III. Office Action Prior Art Rejections

In paragraphs (1)-(2), the Office Action rejected claims 1-19 under 35 U.S.C § 103(a) as unpatentable over Benson, EP 0936530 (Benson) in view of Gabrielle, "USB Forum Produces Logo, Awareness Initiatives, 1997, Computer Retail Week, n 192, pg49" (Gabrielle). Applicants respectfully traverse these rejections.

<u>With Respect to Claim 1</u>: Claim 1 recites:

> *a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol;*

-8-

G&C 30074.27-US-I1

an interface processor, communicatively coupled to the USB-compliant interface and to smartcard processor-compliant interface the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

According to the Office Action, the Benson reference discloses a token having a smart card processor as follows:

> As opposed to a physical smart card reader, a virtual smartcard reader 5 is virtual hardware acting as an emulator that passes information to and from a Virtual Smart Card 6. Additionally, the Virtual Smart Card Reader 5 communicates with a Virtual Smart Card Server 8 (VSC Server) via a network 7, e.g., an Intranet, Extranet, or the Internet. (col. 6, lines 38-45)

> The VSC Server 8 stores all protected information in its database (encrypted using the respective protection keys). When a Virtual Smart Card owner inserts a Virtual Smart Card 6, the VSC server 8 downloads the protected information; and when the owner removes a Virtual Smart Card 6, the Virtual Smart Card 6 uploads the updated protected information to the VSC Server 8. (col. 6, line 38 through col. 7, line 5)

The Applicants respectfully disagree. The foregoing passages do not disclose a personal token having a smartcard processor, but rather, a Virtual Smart Card (VSC), which is essentially a smartcard emulator. The Gabrielle reference likewise fails to disclose a token having a smartcard processor. On this basis alone, the rejection under 35 U.S.C. § 103(a) is improper and should be withdrawn.

The Benson reference likewise fails to disclose the token's interface processor and translation module, which interprets USB-compliant messages into smartcard processor-compliant messages and interprets smartcard-compliant messages into USB-compliant messages. According to the Office Action, the Benson discloses these features as follows:

> The VSC Server then permits the owner to use the Virtual Smart Card. When the Virtual Smart Card owner performs a remove operation, the Virtual Smart Card disables itself, securely sends a remove request to the VSC Server, and then shuts itself down. When the VSC Server receives a remove request, the VSC Server resets the Virtual Smart Card's state in the database to be idle.
> An alternative to the communication between the Virtual Smart Card and the Virtual Smart Card Server is presented in claim 10. The Virtual Smart Card Reader communicates with a dongle (or some other duplication-protected physical media). A duplication protected physical media has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media. The Virtual Smart Card is a copy protected program that executes only if permitted by the Dongle. If the end-user attaches the Dongle to the machine, then the Virtual Smart Card executes; otherwise, the Virtual Smart Card stops. (col 4, lines 4-23).

and

-9-

G&C 30074.27-US-I1

Insert 104: The end-user attaches the dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16).

The foregoing describes the interaction between a the Virtual Smart Card and the Virtual Server (or, in col. 24, a Dongle). It does not describe a token with an interface processor, and does not describe an entity that is coupled between a smartcard processor and a USB-compliant interface, and does not describe any entity that interprets USB-compliant messages into smartcard-compliant messages or smartcard-compliant messages to USB-compliant messages. The Gabrielle reference is likewise deficient.

The Applicants also respectfully disagree that there is any teaching to combine the Benson and Gabrielle references. Although the Office Action indicates that the USB-compliant interface can transfer data quicker than a serial or parallel port, Benson teaches that the Virtual Smart Card and the Virtual Smart Card Server are performed via a network, an Intranet, Extranet, or the Internet (see col. 6, lines 43-45) all of which offer quicker data transfer than a USB-compliant interface.

Accordingly, the Applicants respectfully traverse the rejection of claim 1.

<u>With Respect to Claim 2</u>: Claim 2 recites:

...wherein the interface processor emulates a smartcard reader to the smartcard processor.

According to the Office Action, Benson discloses that the interface processor emulates a smartcard reader to the smartcard processor as follows:

The invention presents a bridge technology called Virtual Smart Card which emulates a real smart card by providing an identical interface and collection of services. *However, the Virtual Smart Card has no physical manifestation.* Any smart card-aware application can seamlessly inter-operate with either a real smart card or a Virtual Smart Card. (col. 3, lines 22-28, emphasis added)

and

The Virtual Smart Card Reader communicates with a Dongle (or some other duplication-protected physical media). A duplication-protected physical media has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media. The Virtual Smart Card is a copy protected program that executes only if permitted by the Dongle. If the end-user attaches the Dongle to the machine, then the Virtual Smart Card executes; otherwise, the Virtual Smart Card stops. (col. 4, lines 14-23)

-10-

G&C 30074.27-US-I1

and

> As opposed to a physical smart card reader, a Virtual Smart Card Reader 5 is a virtual hardware acting as an emulator that passes information to and from a Virtual Smart Card 6. Additionally, the Virtual Smart Card Reader 5 communicates with a Virtual Smart Card Server 8 (VSC Server) via a network 7, e.g. an Intranet, Extranet, or the Internet. (col. 6, lines 38-44)

However, the VSC Reader disclosed above merely forwards emulated smart card messages unchanged to the VSC Server ... it does not "interpret USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages", as claim 2 recites. Accordingly, the Applicants respectfully traverse the rejection of claim 2.

<u>With Respect to Claim 3</u>: Claim 3 recites that:

> *the host processing device comprises a virtual smartcard reader ... including a communication module for packaging messages for transmission to the personal token via the USB compliant interface according to a first protocol and for unpackaging messages received from the personal token via the USB-compliant interface according to the first protocol; and*
> *the interface processor translation module unpackages messages from the host processing device according to the first protocol and packages messages destined for the host processing device according to the first protocol.*

According to the Office Action, the Benson reference discloses a virtual smartcard reader. The Office Action concedes that the Benson reference does not disclose a "communication module for packaging messages for transmission to the personal token via the compliant interface according to a first protocol" but asserts that this communication module is inherently disclosed.

The Applicants respectfully disagree. Benson's Virtual Smart Card Reader interfaces directly with the Virtual Smart Card. Since both the reader and the smart card itself emulate smartcard processes and messages, there is no reason whatsoever for any sort of translation or packaging.

Inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Continental Can Co. v Monsanto Co*, 948 F.2d 1264, 1269(Fed. Cir. 1991). Instead, to establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co*, 948 F.2d at 1268.

-11-

Because there is no reason to include the functionality that the Office Action asserts is inherently disclosed, the Benson reference cannot inherently disclose the features of claim 3. Accordingly, the Applicants respectfully traverse the rejection of claim 3.

With Respect to Claims 4 and 10: Claim 4 recites that the virtual smartcard reader comprises a bootup module for responding to operating system bootup procedures with an indication that a smartcard reader is communicatively coupled to the host processor. According to the Office Action, relying on the following text passage, contends that this is inherently disclosed:

> Insert 104: The end-user attaches the Dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16)

All the foregoing discloses, however, is a bootup procedure for using the smartcard emulation (running on the user's computer) with a dongle. This does not suggest, even inherently, a bootup module, running in the host processing device (analogous to the VSC Server). Accordingly, the Applicants respectfully traverse the rejection of claim 4.

Claim 10 recites analogous features as claim 4 and is patentable for the same reasons.

Regarding claims 6, 12, and 17: Claim 6 recites that the virtual smartcard reader (running in the host processing device) comprises a reporting module for receiving and reporting the insertion of the personal token in a USB-compliant port and the removal of the personal token as a removal of a smartcard from a smartcard reader. According to the Office Action, Benson discloses these features as follows:

> Insert 104: The end-user attaches the Dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16)

> At any time after successfully performing an insert operation, a Virtual Smart Card 6 may perform the remove operation (using the protected channel established during the insert operation). First, the Virtual Smart Card 6 disables itself by refusing all requests for services. Next, the Virtual Smart Card 6 sends a remove request to the VSC Server * which uploads the protected information (encrypted using the protection key). Upon receipt of a remove request, the VSC Server 8 resets its corresponding database entry to idle and returns a success acknowledgement. Next, the Virtual Smart Card 6 unlocks the local machine lock, zeros out the protected information, and shuts itself down. (col. 13, lines 41-53)

-12-

G&C 30074.27-US-I1

Instead of communicating with the Virtual Smart Card Server 8, the Virtual Smart Card Reader 5 communicates with duplication-protected physical media, e.g., a Dongle 1101. (col. 23, lines 34-37)

Remove 105: The Dongle 1101 fails to authorize the Virtual Smart Card 6. For example, the end-user either removes the dongle 1101, or the Virtual Smart Card 6 shuts down. The state is idle 101 after the Dongle 1101 is removed. (col. 24, lines 18-22).

From what the Applicants can ascertain, nothing in the foregoing passage discloses a virtual smartcard reader having a reporting module reporting the insertion of the personal token in USB in a USB-compliant port and the removal of the personal token as a removal of a smartcard from a smartcard reader. At best, the foregoing independently describes a virtual smartcard performing remove operations and sending remove requests, and that the Virtual Smart Card shuts down if the user removes the dongle. Claim 12 is patentable for the same reasons. Accordingly, the Applicants traverse the rejection of claims 6 and 12.

Regarding Claims 7, 13, and 18: Claim 7 recites that *"the virtual smartcard reader further comprises a protocol selection module for receiving a protocol type selection (PTS) command from the operating system and providing a PTS response message to the operating system."* According to the Office Action, Benson inherently discloses this feature because "the virtual smart card can be inserted into different machines." Inherency "may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Continental Can Co. v Monsanto Co.*, 948 F.2d 1264, 1269 (Fed. Cir. 1991). Instead, to establish inherency, the extrinsic evidence "must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill." *Continental Can Co.*, 948 F.2d at 1268. No such showing is possible because the "virtual smart card" is in fact, a software program, running on the user's computer, and is not "inserted into different machines" as the Office Action suggests.

Regarding Claim 8: Claim 8 recites:

a virtual smartcard reader module stored in the memory and in communication with the operating system, for emulating at least one smartcard reader to the operating system, the virtual smartcard reader module comprising a communication module for packaging smartcard-compliant commands for transmission to a personal token communicatively coupled to the host processor via a USB-compliant interface and for unpacking smartcard-compliant responses received from the personal token

-13-

According to the Office Action, these features are disclosed as follows:

> As opposed to a physical smart card reader, a virtual smartcard reader 5 is virtual hardware acting as an emulator that passes information to and from a Virtual Smart Card 6. Additionally, the Virtual Smart Card Reader 5 communicates with a Virtual Smart Card Server 8 (VSC Server) via a network 7, e.g., an Intranet, Extranet, or the Internet. (col. 6, lines 38-45)

> The VSC Server 8 stores all protected information in its database (encrypted using the respective protection keys). When a Virtual Smart Card owner inserts a Virtual Smart Card 6, the VSC server 8 downloads the protected information; and when the owner removes a Virtual Smart Card 6, the Virtual Smart Card 6 uploads the updated protected information to the VSC Server 8. (col. 6, line 38 through col. 7, line 5)

The Applicants respectfully traverse this rejection. As described above with respect to claim 3, Benson does not disclose a virtual smartcard reader having a communication module packaging smartcard compliant commands to a personal token. As disclosed in Benson as follows, the "dongle" is used to authorize the execution of the Virtual Smart Card program:

> Figure 15 illustrates an alternative implementation of the Virtual Smart Card 6. This implementation does not require a VSC Server 8.
> Instead of communicating with the Virtual Smart Card Server 8 the Virtual Smart Card Reader 5 communicates with duplication-protected physical media, e.g., a Dongle 1101. A duplication protected physical media 1101 has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media 1101. The Virtual Smart Card 6 is a copy protected program that executes only if permitted by the Dongle 1101. If the end-user attaches the Dongle 1101 to the machine, then the Virtual Smart Card 6 executes; otherwise, the Virtual Smart Card 6 stops.(col. 23, lines 31-44)

Further, smartcard commands are not sent to either the Virtual Smart Card Server or the dongle. Instead, these entities act only as data repositories where protected data is stored and retrieved. There is no teaching to translate or package smartcard commands or responses. For the foregoing reasons, the Applicants respectfully traverse the rejection of claim 8.

<u>With Respect to Claims 14 and 15</u>: According to the Office Action, claims 14 and 15 are not allowable for the same reasons as claims 1 and 3. The Applicants respectfully traverse for the reasons described with respect to claims 1 and 3. Claim 15 also recites features not recited in claim 3 and is allowable on this basis as well.

<u>With Respect to Claim 16</u>: According to the Office Action, the Benson reference teaches the steps of accepting a startup query from the host computer operating system in the virtual smartcard reader, and providing an indication that a smartcard reader is

-14-

G&C 30074.27-US-I1

communicatively coupled to the host computer to the host computer operating system as follows:

> Insert 104: The end-user attaches the dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16).

The Applicants respectfully disagree that the foregoing discloses anything related to the acceptance of a smartcard query.

<u>With Respect to Claim 19</u>: Claim 19 recites:

> *A virtual smartcard reader emulator system, comprising:*
> *a first smartcard reader emulator, implemented in a host computer for emulating smartcard reader operations to the host computer; and*
> *a second smartcard reader emulator, implemented in a personal key, for emulating smartcard reader operations to a smartcard-interface compliant personal key processor.*

According to the Office Action, the foregoing features are discloses as follows:

> The Virtual Smart Card Reader communicates with a Dongle (or some other duplication-protected physical media). A duplication-protected physical media has the property that it is exceedingly difficult for an unauthorized attacker to construct a copy of the media. The Virtual Smart Card is a copy protected program that executes only if permitted by the Dongle. If the end-user attaches the Dongle to the machine, then the Virtual Smart Card executes; otherwise, the Virtual Smart Card stops. (col. 4, lines 14-23)

and

> Insert 104: The end-user attaches the Dongle 1101 and boots the Virtual Smart Card 6 program. The Virtual Smart Card 6 program does not operate unless the Virtual Smart Card 6 program can validate that the Dongle 1101 is present. The state of the Virtual Smart Card 6 is in-use 102 after the Virtual Smart Card 6 detects the Dongle 1101. This state is not explicitly recorded as in the case with the VSC Server 8. (col. 24, lines 8-16)

Of course, nothing in the foregoing text suggests a smartcard reader emulator in a personal key for emulating smartcard reader operations to a smartcard-compliant personal key processor. Accordingly, the Applicants traverse the rejection of claim 19.

-15-

IV.   Dependent Claims

Dependent claims 2-7, 10-13, and 15-18 incorporate the limitations of their related independent claims, and are therefore patentable on this basis. In addition, these claims recite novel elements even more remote from the cited references. Accordingly, the Applicants respectfully request that these claims be allowed as well.
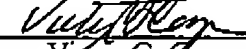
V.   Conclusion

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

GATES & COOPER LLP
Attorneys for Applicant(s)

Howard Hughes Center
6701 Center Drive West, Suite 1050
Los Angeles, California 90045
(310) 641-8797

Date: January 6, 2004

By: _____
Name: Victor G. Cooper
Reg. No.: 39,641

VGC/sjm

-16-

G&C 30074.27-US-I1